Emerging Security Challenges in Highly Interconnected Semiconductor Systems

Neeraj Paliwal
Why Does Security Matter Even More Today?

- Increased complexity and fragility of the supply chain driven by emerging suppliers and technologies such as 3D chips and systems, (multi-) chiplet integration, stacking etc.,

- Exponential increase of data acquisition rate per sensor. Total data acquisition has been estimated to reach $10^{27}$ bytes-per-year by 2032 (>10^20 bit/s)

- Paradigm shift from "move data to compute" to "move compute to data" driven by the alarming growing gap between the world’s technological informational storage need and the communication capacity
Why Does Security Matter Even More Today?

Moore’s law is slowing

General purpose CPUs and GPUs can’t meet the performance demands of today’s AI workloads

AI workload optimized “heterogeneous compute” architecture is driving the demand for new chips

These new chips are developed by emerging system design companies instead of the traditional ones

Many designs focus on AI performance and may find their chips vulnerable without a reliable IP supplier
Emerging Trends: From Data Centers to DATA Everywhere

Exponential growth of recorded data at the edge

Only 25% of the acquired data will be housed in a data center

Communication backbone e.g., 5G

A paradigm shift is required to admit data at the edge into economic activity:
- Move the compute to the data
- Security in the broadest sense: Protection, Trust and Control

Total-data acquisition has been estimated to reach $10^{27}$ bytes-per-year by 2032
AI Capabilities: From Cloud to Edge

**Cloud systems**

- Significant shift of decision-making tasks from cloud to edge enabled by AI components

**Edge**

- IoT edge devices
- Cyber-physical systems
- Personal augmentation devices

**Demand on continuous evolution of data analytics**

- Secure over the air updates
- Data attestation
- Secure integration and deployment regimes

**AI/ML models & inference value**
Security at the Edge: Challenges

• Edge devices are in the field
  • Easier to access for adversaries
  • Non-expert users
    • Devices are supposed to help / entertain, not create work
  • Wide-ranging environment interactions
    • Example: Troop locations revealed by fitness trackers

• Governments have taken notice: Regulation
  • Privacy (e.g., GDPR)
  • Health (e.g., HIPAA Security Rule)
  • Automotive Cyber Security (e.g., UNR 155 & 156)
  • US National Cyber Security Strategy
  • EU Cyber Security Act & EU Cyber Resilience Act
  • Government purchasing requirements (e.g., FISMA, EO14028)
Traditional Security is the Basic Layer at the Edge

- Securing cryptographic keys
  - ✓ Root of Trust
  - ✓ Secure Element
- Securing firmware and over the air updates
  - ✓ Secure boot
  - ✓ Package / update managers, signed updates
- Securing IDs
  - ✓ Biometrics
  - ✓ Password managers
- Secure development processes
  - ✓ Limit attack surface by fighting feature creep
  - ✓ Vulnerability scanners and vulnerability disclosure routines
  - ✓ Established, high quality code base (libraries)
A Very High-Level View of Shor’s Quantum Algorithm

- To break RSA, we need to learn secret primes $p, q$ from public $N$ (we know $N = pq$)
- From number theory, we know that for suitable $x$, $r \equiv x^y \mod N$ is periodic
  - i.e., $r \equiv x^y \mod N \equiv x^{y+\phi} \mod N \equiv x^{y+2\phi} \mod N \equiv \ldots$
- From number theory, we further know that $\phi \in \{1, p - 1, q - 1, (p - 1)(q - 1)\}$
- Quantum superposition enables (relatively) efficient Quantum Phase Estimation (QPE)
- Quantum Fourier Transform (QFT) allows extracting binary integer $\phi$ from QPE results
- Small number of repetitions needed until suitable $x$ found
Updating the Traditional Security: Quantum-Secure Crypto

- Quantum Computers threaten RSA, ECC
  - Digital signature algorithms must change
  - Session key establishment algorithms must change
- Use cases determine when the change must happen
  - Mosca’s Theorem: Everything is good as long as \( t_u + t_s < t_q \)
    - \( t_u \): Time to update devices, networks and applications
    - \( t_s \): Time that data needs to be secure
    - \( t_q \): Time until quantum computers large enough
- Transition to Quantum Secure Crypto is a massive effort
  - All IoT devices / services will be affected
  - Governments around the world push to hasten transition
- Standardization in progress but no standards yet
  - Except for secure boot (LMS, XMSS)

Rapidly evolving situation – challenging everyone for the next 15 years
Physical Attacks at the Edge

• Service interruption
  • Disrupting cables, wireless is cheap
  • Need to plan infrastructure with human adversaries in mind

• Side-channel attacks
  • Measure power / EM / time / … of computation
  • “Look inside” operations, exploit sensitive intermediates
  • More powerful than normal adversaries

• Targeted fault-injection attacks
  • Authentication bypass (e.g., ID and firmware checks)
  • Key extraction (e.g., faulted cryptographic operations)
  • Data dumps (e.g., pointer manipulation)
  • Can even abuse device features like power scaling

Robust knowledge foundations but most markets only catching up.
Security at the Edge: Attacking AI

- Artificial Intelligence derived from biological models
  - Natural intelligences can be tricked – used for education, psychological healing, marketing, abuse
  - No inherent countermeasures against malicious inputs in AI either

- At edge, additional attacks are possible
  - Proprietary AI models are a form of content that requires protection against pirates
  - Content pirates know how to use side-channel attacks
  - Content pirates know how to use fault-injection attacks
  - AI models increasingly mission critical – denial of service particularly easy at edge

Ongoing research topic
Security at the Edge: Securing Computations

At the edge, you find:

- Proprietary data from multiple sources
- Proprietary analysis algorithms processing data
- Vulnerable devices

Advanced cryptography provides solution:

- Fully-Homomorphic Encryption (FHE)
- Multi-Party Computation (MPC)

Basic idea: Compute only on encrypted data
Basic idea: Use cryptographic means to scramble algorithms

Current situation: Practicality of schemes very use-case specific
Current situation: Limited useability, expert knowledge required
Current situation: First deployments in networking, ad auctions, genome research

Emerging technology, not ready for general purpose deployments yet.
Security at the Edge: Securing Sensors

• For car keys: long history of distance bounding solutions and attacks
  • Relay attacks allow adversaries to unlock cars even if key is far away
  • Distance bounding tries to ensure that key is near car
  • Basic idea: derive distance measurement from response times
  • Current situation: Cat-and-mouse between defenders and adversaries

• Fundamental problem:
  • Cryptography is mathematical, measurements are physical
  • Cryptography derives its strength from reductions to mathematically “hard” problems
  • Measurements for IoT can not be reduced to physical equivalent of “hard” problem
  • Any IoT sensor will can be fooled by sufficiently motivated engineer
  • Faulty sensor inputs will always be a problem for AI in IoT
Summary

• Compute and data are moving into highly interconnected edge devices
$ Edge devices are increasingly driving business critical applications
✓ We can deploy solid basic security for edge devices
! But risks are larger due to edge exposure and basic security is not enough
  o Many challenges are work in progress
  o AI at the edge adds its own challenges
  o Advanced cryptography is providing new opportunities
  o Need to account for risks that cryptography can not solve
Thank you